

07-21-00

A

EK 25738488545

THE ASSISTANT COMMISSIONER FOR PATENTS
Washington, D.C. 20231

DOCKET NUMBER: AUS990912US1

DATE: 07/20/2000

Sir:

Transmitted herewith for filing is the Patent Application of:

Inventors: **William J. Reid**

For: **System, Apparatus and Method for Updating Security Configurations of a Plurality of Servers from a Centralized Directory Server**

Enclosed are:

☒ Patent Specification and Declaration☒ 5 sheets of drawing(s). (Informal)☒ An assignment of the invention to International Business Machines Corporation (includes Recordation Form Cover Sheet).☐ A certified copy of a ☐ application.☐ Information Disclosure Statement, PTO 1449 and copies of references.☒ Declaration Under 37 C.F.R. 1.47b

The filing fee has been calculated as shown below:

For	Number Filed	Number Extra	Rate	Fee
Basic Fee				\$760.00 690.00
Total Claims	40 - 20	20	x 18 =	\$360.00
Indep. Claims	5 - 3	2	x 78 =	\$156.00
MULTIPLE DEPENDENT CLAIM PRESENTED			x 260 =	\$ 0.00
			TOTAL	\$1206.00

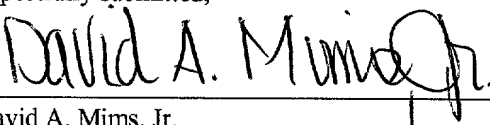
☒ Please charge my Deposit Account No. 09-0447 in the amount of \$1206.00. A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account 09-0447. A duplicate copy of this sheet is enclosed.

☒ Any additional filing fees required under 37 CFR 1.16.☒ Any patent application processing fees under 37 CFR 1.17.

Respectfully submitted,

By



David A. Mims, Jr.
Registration No. 32,708
Intellectual Property Law Dept.
IBM Corporation
11400 Burnet Road, Zip 4054
Austin, Texas 78758
Telephone (512) 823-0950

07/20/00
jc848 U.S. PTO

jc598 U.S. PTO
09/620350
07/20/00

00620350-072000

Docket No. AUS990912US1

**System, Apparatus and Method for Updating
Security Configurations of a Plurality of
Servers from a Centralized Directory Server**

5

BACKGROUND OF THE INVENTION

1. Technical Field:

10 The present invention is directed to a system,
apparatus and method for updating security configurations
of a plurality of servers from a centralized directory
server.

2. Description of Related Art:

15 As businesses and organizations grow in size, their
computer networks also grow to accommodate the increasing
workload. It is not unusual for large businesses and
organizations to have hundreds or thousands of network
servers located in many different geographical locations.
20 As the computer networks increase in size, security
issues become more of a problem.

For example, many computer networks make use of
Windows NT Servers, available from Microsoft Corporation,
which provide resources and store files for use by users
25 of the computer network. The resources and files of the
Windows NT Servers have access control lists (ACLs)
associated with them. An ACL is a set of data associated
with a file, directory or other resource that defines the
permissions that users and/or groups have for accessing
30 it.

As the computer network grows in size, the number of
servers and resources/files on the computer network
increase. A user may be granted access to
resources/files on a large number of the servers of the

Docket No. AUS990912US1

computer network. If a user's access to the computer network is changed, each server of the computer network must be updated to reflect the user's new access. Such updates require that the ACL of each file on each server
5 of the computer network to which the user had access and the ACL of each file on each server to which the user will be granted access, be updated.

The current manner in which this access update is accomplished is to have a human network administrator log
10 onto each server individually and update the ACLs to reflect the user's new access. When the computer network has grown to a large size, such updates become impractical. As a result, many businesses and organizations do not make use of the ACLs or do not
15 update them to reflect changes in user access. As a result a serious security problem arises. Thus, it would be advantageous to have a system, apparatus and method for updating security configurations of a plurality of servers from a centralized location.

20

SUMMARY OF THE INVENTION

5 The present invention provides a system, apparatus
and method for updating the security configurations of
servers from a centralized directory server. With the
present invention, when a change needs to be made to the
authorized users of the servers, the change is first
10 registered with a centralized directory server. The
changed attribute(s) is then downloaded to the servers
and used to update security parameter lists associated
with each file to which the user's access has changed.
By downloading the changed attribute, either only the
15 user's information whose attribute has changed will be
downloaded or the entire directory listing may be
downloaded to each server for use in updating the
security parameter lists.

20 The downloading of the changed attribute may be
initiated by a system administrator, may be a
periodically initiated event, or by some selected event.
Alternatively, each server may log onto the directory
server and request information to be downloaded from the
directory server. Such log on requests from the servers
25 may be for the entire directory listing or may be for
designated subsections of the directory listing.

30 The downloaded information from the directory server
is used by the servers to update the security parameter
lists for the files and resources of the servers. The
information downloaded from the directory server may be
filtered to obtain only the information used to update
the security parameter lists. The filtering may be

performed by application programs running on either the servers or on the directory server.

In this way, the security parameter lists on each server may be updated without requiring a user or network administrator to log onto each server individually to make the change to each file/resource. Rather, with the present invention, the security parameter lists may be updated from a centralized directory database in a relatively automatic fashion, thereby greatly reducing the burden of maintaining secured network servers.

BRIEF DESCRIPTION OF THE DRAWINGS

5 The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself, however, as well as a preferred mode of use, further objectives and advantages thereof, will best be understood by reference to the following detailed
10 description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 is an exemplary block diagram of a system in which the present invention may be implemented;

Figure 2 is an exemplary block diagram of the
15 directory server of **Figure 1**;

Figure 3 is an exemplary block diagram of a server according to the present invention;

Figure 4 is a flowchart outlining an exemplary operation of the directory server of **Figure 2**; and

20 **Figure 5** is a flowchart outlining an exemplary operation of a server in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

5 **Figure 1** is an exemplary block diagram of a system
100 in which the present invention may be implemented.
As shown in **Figure 1**, the system 100 includes a network
110, a plurality of servers 120-140, and a directory
server 150. Each server 120-140 stores files 160 and
10 provides resources that are accessible by users of the
network 110.

Each file and/or resource of each server 120-140 has
an associated security parameter list 170, such as an
access control list (ACL). The security parameter list
15 170 identifies which users or groups of users are to be
provided access to the associated file. For example, the
security parameter list 170 may include a listing of user
identifiers of authorized users.

The designation of which users or groups of users
20 are given access to a particular file may be made, for
example, by a particular user's system identifier, a
user's name, a user's group identifier, a user's access
security level, and the like. For example, the security
parameter list 170 may indicate that all users of access
25 security level 3 or higher may access a particular file.
Alternatively, the security parameter list 170 may
indicate that John Smith has access to the particular
file or that all users in the "Sales" group are given
access to the file. Any manner of designating authorized
30 users is intended to be within the spirit and scope of
the present invention.

Docket No. AUS990912US1

The directory server **150** stores a directory listing **155** of users of the network **110**. The directory listing **155** may be a flat file, a relational database, or the like. The directory listing **155** includes, for example, a user identifier and various user attributes. The user attributes may include, for example, the user's name, address, contact information, groups to which the user belongs, such as "Sales" or "Research and Development", an access security level, and the like. The directory listing **155** may include more attributes than is used by the security parameter lists **170**.

The servers **120-140** and the directory server **150** communicate with each other over the network **110**. The network **110** may be any type of network for communicating data between data processing devices. For example, the network may be a local area network (LAN), a wide area network (WAN), the Internet, an intranet, wireless communication network, satellite communication network, and the like. Furthermore, the network **110** may be a plurality of networks of the same or different types.

The servers **120-140** and the directory server **150** may communicate with one another using any known or later developed protocol, as is readily apparent to those of ordinary skill in the art. For example, the servers **120-140** and the directory server **150** may communicate over the network **110** using the telnet protocol, light weight directory access protocol (LDAP), transfer control protocol (TCP)/Internet Protocol (IP), and the like.

When a change needs to be made to the authorized users of the network **110** and/or the servers **120-140**, the change is first registered with the directory server **150**.

Docket No. AUS990912US1

For example, if a user of the network 110 is transferred from a first group, e.g. "R&D", to a second group "Sales", the files to which the user is provided access may need to be changed so that the user is provided
5 access to files he/she did not have access to and the user's access is removed from files that he/she should no longer have access to.

The change is first made to the directory listing **155** in the directory server **150**. The update to the
10 directory listing in the directory server **150** may be made, for example, by logging onto the directory server **150** and using an editor or other server application to edit the directory listing **155**. For example, an editor may be used to search the directory listing for a
15 particular user identifier and then to edit the attributes associated with the user identifier.

The changed attribute is then downloaded to the servers **120-140** and used to update the security parameter lists **170** associated with each file to which the user's
20 access has changed. By downloading the changed attribute, either only the user's information whose attribute has changed will be downloaded or the entire directory listing may be downloaded to each server **120-140** for use in updating the security parameter lists
25 **170**.

The downloading of the changed attribute may be initiated by the system **100** administrator, periodically, or by a selected event, such as whenever a change to an attribute is made. Thus, for example, after entering the
30 changed attributes of various users in the directory listing **155**, the system **100** administrator may enter a

Docket No. AUS990912US1

command to the directory server **150** instructing the directory server **150** to download the directory listing **155** or only the user information for the users having changed attributes, to the servers **120-140**.

- 5 Alternatively, the system **100** administrator may make the necessary changes tot he directory listing **155** and have the changes downloaded to the servers **120-140** at the next scheduled update of the security parameter lists **170**.

In another implementation, each server **120-140** may
10 log onto the directory server and request information to be downloaded from the directory server **150**. Such log on requests from the servers **120-140** may be for the entire directory listing **155** or may be for designated subsections of the directory listing **155**. For example,
15 if a file is to be accessed by all users having level 3 or higher security, the log on request may request only information for those users that have level 3 security or higher from the directory listing **155**.

The downloaded information from the directory server
20 **150** is used by the servers **120-140** to update the security parameter lists for the files and resources of the servers **120-140**. The information downloaded from the directory server **150** may be filtered to obtain only the information used to update the security parameter lists
25 **170**. The filtering may be performed by application programs running on either the servers **120-140** or on the directory server **150**.

In this way, the security parameter lists **170** on each server **120-140** may be updated without having to log
30 onto each server individually. Rather, with the present

invention, the security parameter lists **170** may be updated from a centralized directory database **150**, thereby greatly reducing the burden of maintaining secured network servers.

5 **Figure 2** is an exemplary block diagram of the directory server **150**. As shown in **Figure 2**, the directory server **150** includes a controller **210**, a network interface **220**, a directory storage device **230**, a memory and an input interface **250**. These devices are in
10 communication with one another via the control/signal bus **260**. While **Figure 2** shows a bus architecture, other architectures, as will be readily apparent to those of ordinary skill in the art, may be used without departing from the spirit and scope of the present invention.

15 The controller **210** controls all the operations of the directory server **150** based on instructions stored in the memory **240**. The directory storage device **230** stores the directory listing **155**. The controller **210** sends and receives communications over the network **110** via the
20 network interface **220**.

The controller **210** may also receive input, such as changes to the directory listing **155**, via the input interface **250**. The input interface **250** may include an editor application through which a network administrator
25 or the like, may edit the directory listing **155** stored in the directory storage device **230**. The editor application may be stored, for example, in memory **240** and executed by the controller **210** when updates to the directory listing **155** are needed.

30 When instructed by the network administrator via the

Docket No. AUS990912US1

input interface **250**, at scheduled periodic times, and/or when receiving a request from a server, such as servers **120-140**, via the network interface **220**, the controller **210** initiates a transmission of appropriate directory listing **155** data from the directory storage device **230** to the servers **120-140** via the network interface **220**. The appropriate directory listing **155** data may include the entire directory listing **155**, only those entries in the directory listing that have been changed, or those entries meeting criteria set by a request from the servers **120-140**.

The transmission of the appropriate directory listing **155** is received by one or more of the servers **120-140** and used to update the security parameter listings of the files and resources stored on the server(s) **120-140**.

Figure 3 is an exemplary block diagram of a server, such as server **120**, for example. As shown in **Figure 3**, the server **120** includes a controller **310**, a network interface **320**, a storage device **330**, a memory **340**, and a security update device **350**. These devices are in communication with one another via the control/signal bus **360**. Although a bus architecture is shown in **Figure 3**, other architectures, as will be readily apparent to those of ordinary skill in the art, may be used without departing from the spirit and scope of the present invention.

The transmission of directory listing **155** information is received by the server **120** via the network interface **320**. The controller **310**, operating based on

Docket No. AUS990912US1

instructions stored in memory **340**, directs the received information to the security update device **350**. The received information may be temporarily stored in storage device **330** for use by the security update device **350**.

5 The security update device **350** may filter the received information for the information necessary to update the security parameter lists **170**. The filtering may be performed, for example, based on field identifiers or tags included in the received information. For
10 example, each data segment may be identified by a tag that indicates the classification of the data segment is. For example, a tag may indicate that the data segment identifies a security level of an authorized user, a security group of the authorized user, an address for the
15 authorized user, and the like. The security update device **350** may filter the received information and select the data segments that are necessary to update the security parameter lists **170**. Other methods of filtering the received information for the necessary data segments
20 may be used without departing from the spirit and scope of the present invention.

Furthermore, rather than performing the filtering of directory listing information at the server **120**, the filtering may be performed prior to transmission of the
25 information by the directory server **150**. For example, the directory server **150** may select data segments from the directory listing **155** for transmission to the servers **120-140**. If the information is filtered by the directory server **150**, filtering may not be necessary at the servers
30 **120-140**. However, a server **120**, for example, may also perform filtering functions if the necessary information

Docket No. AUS990912US1

for the server **120** differs from the necessary information for the other servers **130-140**.

Once the received information is filtered for the necessary information, either by the directory server **150**, the server **120**, or both, the security update device **350** may update the security parameter lists **170** associated with the files/resources stored in the storage device **330**. The security update device **350** modifies the data in the security parameter lists **170** in accordance with the received information and stores the modified security parameter list **170** in the storage device **330**.

For example, assume that the received information indicates that a new user has been added to the system **100** and that the new user has an access level of 2. When the received information is used by the security update device **350** to update the security parameter lists **170**, the security parameter lists **170** of files that are accessible by users with level 2 security will be updated to include the new user's identifier. In this way, the new user is added as an authorized user of the associated files.

Thus, with the present invention, security parameter lists for a multitude of files/resources on a plurality of servers may be updated and maintained from a centralized directory server. Because the update process is relatively automated and controlled from a central location, the update process is greatly simplified over the known systems.

Figure 4 is a flowchart outlining an exemplary operation of the directory server according to the present invention. The operation shown in **Figure 4**

Docket No. AUS990912US1

assumes that updates to the security parameter lists 170 are performed after the directory listing 155 is updated. However, as described above, the update to the security parameter lists 170 may be performed at periodic times or
5 when requested by the servers 120-140.

As shown in **Figure 4**, the operation starts with a directory server, such as directory server 150, receiving changes to a directory listing, such as directory listing 155 in **Figure 1**(step 410). After all necessary changes
10 have been received, the directory server receives an update command (step 420) which may be input, for example, by a network administrator or automatically input on a scheduled periodic basis.

When the directory server receives the update
15 command, the directory server sends directory information to one or more servers, such as servers 120-140(step 430). The directory information sent to the servers may be filtered for only the necessary security parameter list update information, may include only the changed
20 information, may include a subsection of the directory listing, or may include the entire directory listing, based on the type of update command received. The operation of the directory server then ends (step 440).

Figure 5 is a flowchart outlining an exemplary
25 operation of a server, such as server 120, for example. As shown in **Figure 5**, the server receives the directory information from the directory server (step 510). If the directory information has not already been filtered by the directory server or if additional filtering is
30 necessary, the server may filter the received directory information for only the directory information that is

Docket No. AUS990912US1

necessary for updating the security parameter lists, such as security parameter list **170** (step **520**). The resulting update information is then used to update the security parameter lists for each of the files/resources
5 associated with the server (step **530**). The operation then ends (step **540**).

The present invention provides a system, apparatus and method for updating security configurations of a plurality of servers from a centralized directory server.
10 The present invention greatly simplifies the process of updating security parameter lists associated with files/resources of servers in a network by allowing the update to be controlled from a central location. Because the update process is controlled from a central location
15 and is relatively automatic, the speed and ease with which the updates are performed is increased, thereby increasing the overall security of the system.

While the present invention has been described with reference to a single directory server **150** facilitating
20 the updating of security information for a plurality of servers, it should be appreciated by those of ordinary skill in the art that the network **110** may include many hundreds or thousands of servers **120-140** that must be updated. In such a system, it may be impractical to use
25 a single directory server **150** to update all of the hundreds or thousands of servers **120-140**. Thus, a plurality of directory servers, such as directory server **150**, may be included in the network **110**.

With such an embodiment, each directory server **150**
30 will be responsible for updating the servers **120-140** of a particular sub-group of the network **110**. the directory

Docket No. AUS990912US1

server **150** must therefore keep information pertaining to the network identifiers of the servers **120-140** for which it is responsible and use these network identifiers to update the servers **120-140** for which it is responsible.

5 In addition, the directory servers **150** themselves may be updated by a central server, such that a pyramidal hierarchy of servers is created. In this way, the central server may be updated by a network administrator, or the like, the updates may be passed down to each of
10 the directory servers **150**, which in turn may pass the updates down to the servers **120-140**. Other modifications to facilitate such a pyramidal hierarchy may be made without departing from the spirit and scope of the present invention.

15 It is important to note that while the present invention has been described in the context of a fully functioning data processing system, those of ordinary skill in the art will appreciate that the processes of the present invention are capable of being distributed in
20 the form of a computer readable medium of instructions and a variety of forms and that the present invention applies equally regardless of the particular type of signal bearing media actually used to carry out the distribution. Examples of computer readable media
25 include recordable-type media such a floppy disc, a hard disk drive, a RAM, and CD-ROMs and transmission-type media such as digital and analog communications links.

 The description of the present invention has been presented for purposes of illustration and description,
30 but is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and

variations will be apparent to those of ordinary skill in the art. The embodiment was chosen and described in order to best explain the principles of the invention, the practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.

5

Docket No. AUS990912US1

CLAIMS:

What is claimed is:

5

1. A method of updating security configurations of a plurality of servers, comprising:

changing security information in a centralized server;

10

receiving an update command; and

downloading the changed security information to the plurality of servers in response to receiving the update command, wherein the downloaded changed security information is used to update the security configurations of the plurality of servers.

15

2. The method of claim 1, wherein the plurality of servers are Windows NT servers and the centralized server is a directory server.

20

3. The method of claim 1, wherein the centralized server is a directory server and wherein changing the security information includes using an editor to change a directory listing in the centralized server.

25

4. The method of claim 1, wherein the security configurations of the plurality of servers are updated by updating security parameter lists associated with a plurality of files and/or resources associated with each of the plurality of servers.

30

Docket No. AUS990912US1

5. The method of claim 4, wherein the security parameter lists identify authorized users or authorized groups of users of the files and/or resources associated with the security parameter lists.

5

6. The method of claim 1, wherein the update command is received from a network administrator.

7. The method of claim 1, wherein the update command is received at scheduled periodic times.

10

8. The method of claim 1, wherein the update command is received from one or more of the plurality of servers.

9. The method of claim 1, wherein the centralized server is a light weight directory access protocol server.

15

10. The method of claim 1, wherein downloading the changed security information includes filtering a directory listing stored on the centralized server to extract the changed security information.

20

11. The method of claim 1, wherein the security configurations are updated by filtering the downloaded changed security information to extract only necessary update information for updating the security configurations and then updating the security configurations based on the extracted necessary update information.

25

30

12. A security configuration update server for updating

security configurations of a plurality of servers,
comprising:

a network interface coupled to the controller; and

13. The security configuration update server of claim
12, wherein the plurality of servers are Windows NT
15 servers and the security configuration update server is a
directory server.

15. The security configuration update server of claim 12, wherein the security configurations of the plurality of servers are updated by updating security parameter lists associated with a plurality of files and/or resources associated with each of the plurality of servers.

16. The security configuration update server of claim
30 15, wherein the security parameter lists identify
authorized users or authorized groups of users of the
files and/or resources associated with the security

parameter lists.

5

10

15

20

25

30

23. A computer program product in a computer readable medium for updating security configurations of a plurality of servers, comprising:

second instructions for receiving an update command;
and

24. The computer program product of claim 23, wherein the centralized server is a directory server and wherein the first instructions include instructions for using an editor to change a directory listing in the centralized server.

26. The computer program product of claim 25, wherein the security parameter lists identify authorized users or authorized groups of users of the files and/or resources associated with the security parameter lists.

30

27. The computer program product of claim 23, wherein the update command is received from a network

Docket No. AUS990912US1

administrator.

28. The computer program product of claim 23, wherein
the update command is received at scheduled periodic
5 times.

29. The computer program product of claim 23, wherein
the update command is received from one or more of the
plurality of servers.

10

30. The computer program product of claim 23, wherein
the centralized server is a light weight directory access
protocol server.

15 31. The computer program product of claim 23, wherein
the third instructions include instructions for filtering
a directory listing stored on the centralized server to
extract the changed security information.

20 32. A method in a data processing system for updating
access information for a plurality of servers, the method
comprising:

collecting changes to access information at the data
processing system to form modified access information;

25 and

responsive to a policy, transferring the modified
access information to the plurality of servers, wherein
the modified access information is used to update the
security configurations of the plurality of servers.

30

33. The method of claim 32, wherein the policy comprises
receiving a request to update the security configurations

Docket No. AUS990912US1

for the plurality of servers.

34. The method of claim 32, wherein the policy comprises
periodically initiating transfer of modified access
5 information to the plurality of servers.

35. The method of claim 32, wherein the policy comprises
initiating the transfer of the modified access
information to the plurality of servers in response to a
10 selected event.

36. The method of claim 35, wherein the selected event
is a periodic event.

15 37. A data processing system, comprising:
a centralized server; and
a plurality of servers coupled to the centralized
server by at least one network, wherein the centralized
server stores security information, and wherein when the
20 centralized server receives an update command, the
security information stored in the centralized server is
downloaded to at least one of the plurality of servers,
the downloaded security information being used by the at
least one of the plurality of servers to update the
25 security configurations of the at least one of the
plurality of servers.

38. The system of claim 37, wherein the plurality of
servers are Windows NT servers and the centralized server
30 is a directory server.

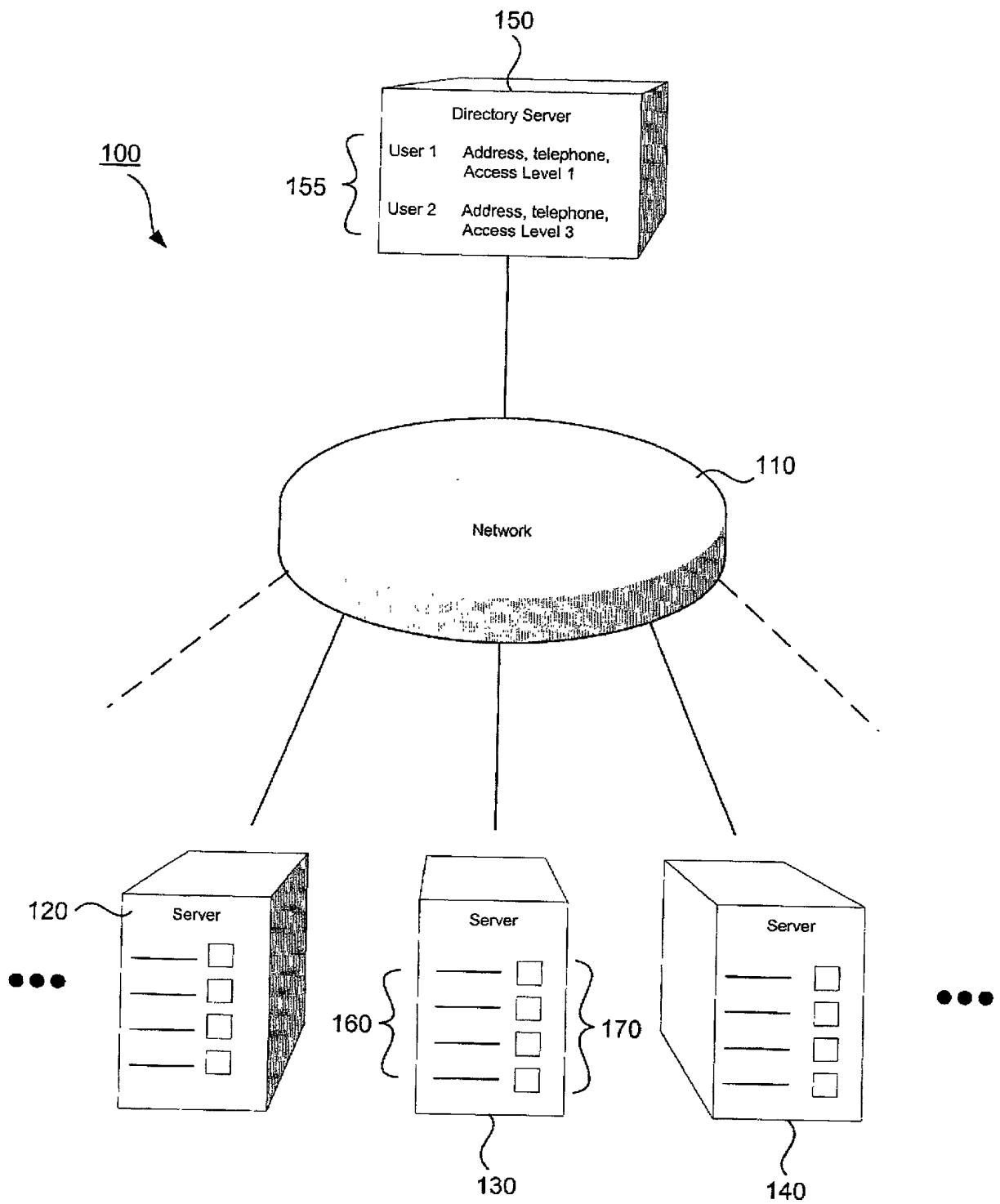
39. The system of claim 37, wherein the security

5

10

System, Apparatus and Method for Updating Security Configurations of a Plurality of Servers from a Centralized Directory Server

A system, apparatus and method for updating security configurations of a plurality of servers from a centralized directory server. The system includes a centralized directory server and a plurality of servers that provide resources and store files for use by users of the system. Each file/resource associated with the servers includes a security parameter list identifying authorized users of the file/resource. The security parameter lists are updated from the centralized directory server by first inputting changes to the system security configuration in the directory server and then downloading these changes to the plurality of servers. The changes are used by the plurality of servers to update the security parameter lists associated with the files/resources of the server.

**Figure 1**AUS990912US1
Sheet 1 of 5

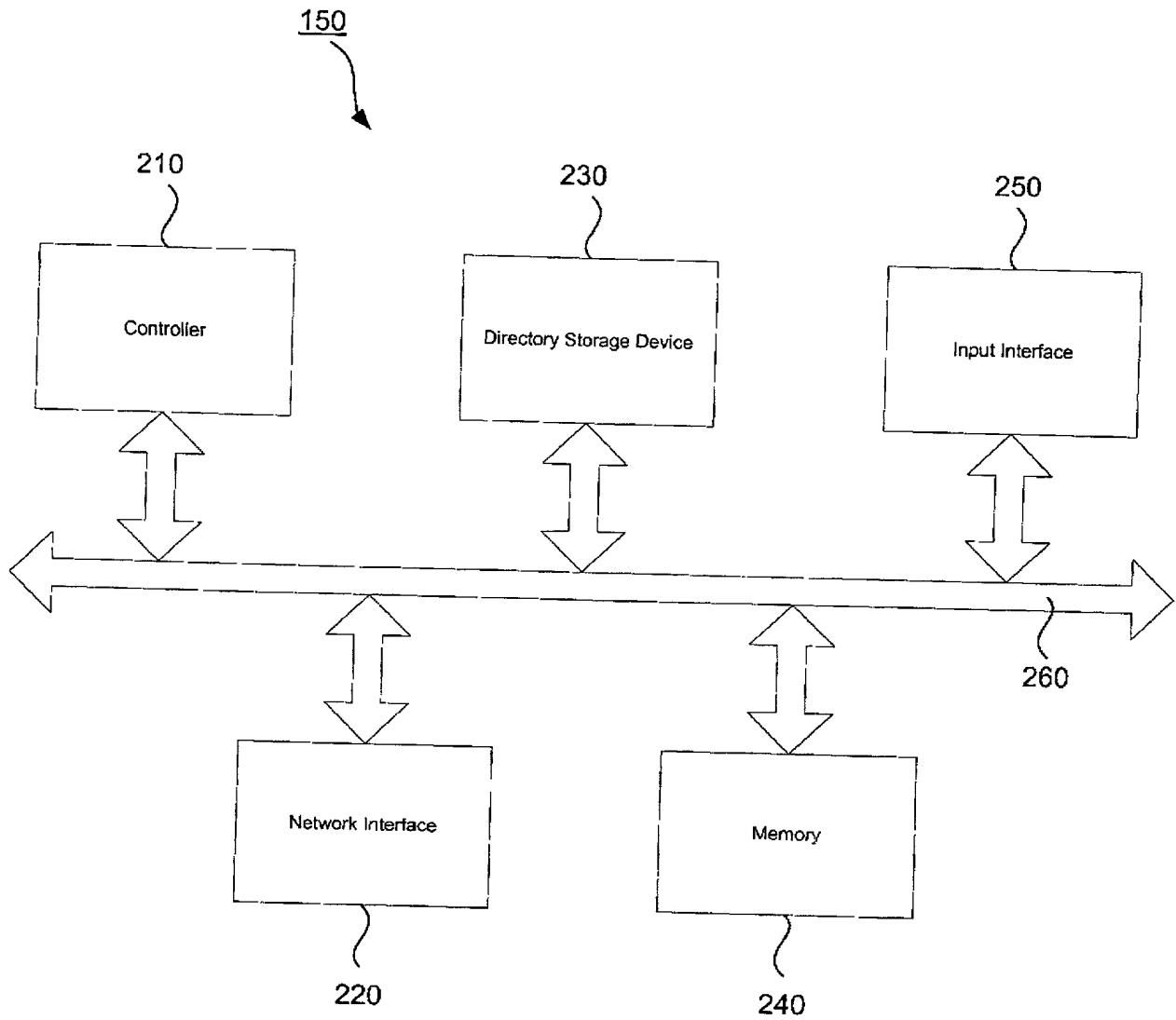


Figure 2
AUS990912US1
Sheet 2 of 5

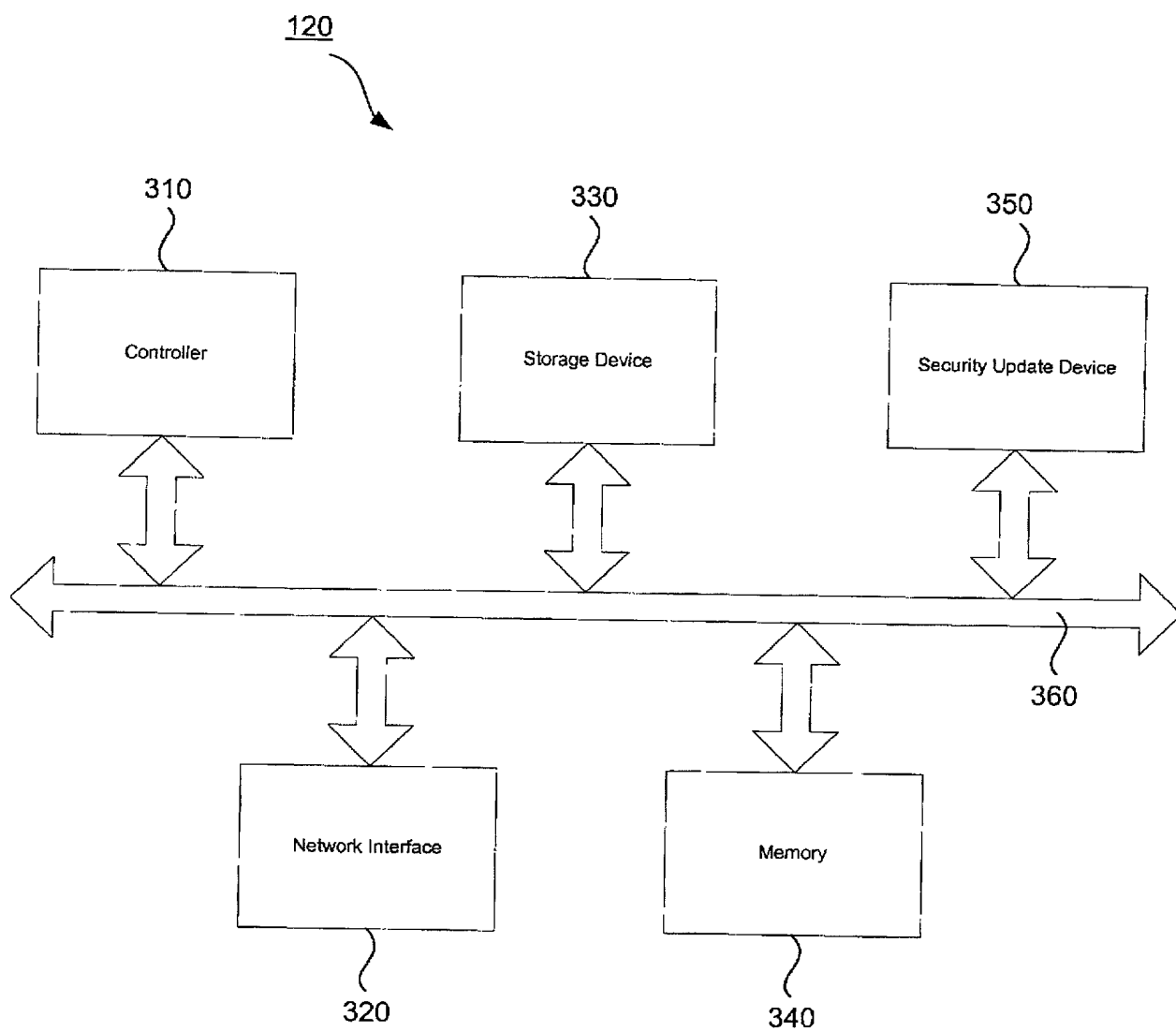


Figure 3
AUS990912US1
Sheet 3 of 5

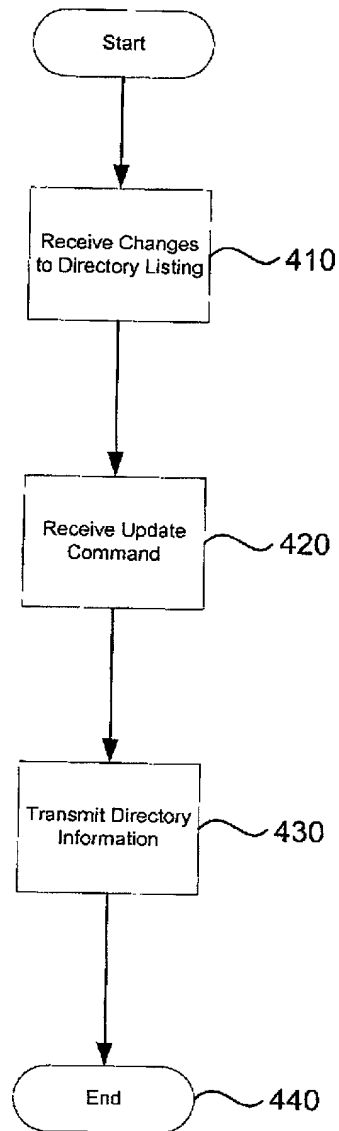


Figure 4
AUS990912US1
Sheet 4 of 5

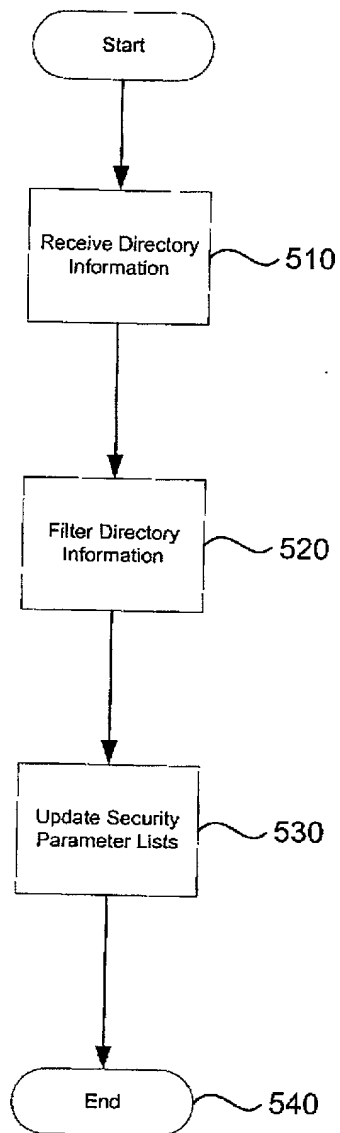


Figure 5
AUS990912US1
Sheet 5 of 5

**DECLARATION AND POWER OF ATTORNEY FOR
PATENT APPLICATION**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

**System, Apparatus and Method for Updating Security Configurations of a
Plurality of Servers from a Centralized Directory Server**

the specification of which (check one)

X is attached hereto.

___ was filed on _____
as Application Serial No. _____
and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s): Priority Claimed
____ Yes ____ No
(Number) (Country) (Day/Month/Year)

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial #) (Filing Date) (Status)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

John W. Henderson, Jr., Reg. No. 26,907; Thomas E. Tyson, Reg. No. 28,543; James H. Barksdale, Jr., Reg. No. 24,091; Casimer K. Salys, Reg. No. 28,900; Robert M. Carwell, Reg. No. 28,499; Douglas H. Lefevre, Reg. No. 26,193; Jeffrey S. LaBaw, Reg. No. 31,633; David A. Mims, Jr., Reg. No. 32,708; Volel Emile, Reg. No. 39,969; Anthony V. England, Reg. No. 35,129; Leslie A. Van Leeuwen, Reg. No. 42,196; Christopher A. Hughes, Reg. No. 26,914; Edward A. Pennington, Reg. No. 32,588; John E. Hoel, Reg. No. 26,279; Joseph C. Redmond, Jr., Reg. No. 18,753; Marilyn S. Dawkins, Reg. No. 31,140; Mark E. McBurney, Reg. No. 33,114; Duke W. Yee, Reg. No. 34,285; Colin P. Cahoon, Reg. No. 38,836; Joseph R. Burwell, Reg. No. 44,468; Rudolph J. Buchel, Reg. No. 43,448; and Stephen R. Loe, Reg. No. 43,757; and Stephen J. Walder, Jr., Reg. No. 41,534.

Send correspondence to: Duke W. Yee, Carstens, Yee & Cahoon, LLP, P.O. Box 802334, Dallas, Texas 75380, and direct all telephone calls to Duke W. Yee, (972) 367-2001.

FULL NAME OF SOLE OR FIRST INVENTOR: William J. Reid

INVENTORS SIGNATURE: _____ DATE: _____

RESIDENCE: _____

CITIZENSHIP: United States

POST OFFICE ADDRESS: SAME AS ABOVE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	:	Before the Examiner:
William Joseph Reid	:	
Serial No.:	:	Group Art Unit:
Filed:	:	Intellectual Property
Title: System, Apparatus and Method	:	Law Department
for Updating Security Configuration of	:	National Business
a Plurality of Servers From A	:	Machines Corporation
Centralized Directory Server	:	11400 Burnet Road
	:	Austin, Texas 78758

July 19, 2000

DECLARATION UNDER 37 C.F.R. 1.47b

Assistant Commissioner of Patents

Washington, D. C. 20231

Sir:

Martha A. Acosta declares as follows:

1. I am currently employed by International Business Machines Corporation ("IBM") in the Intellectual Property Law department.
2. I was assigned the duty by IBM of obtaining the signatures of William J. Reid ("Reid"), whose last known address is 7819 Pencross Lane, Dallas, Texas 75248 and is the inventor for a patent application entitled "System, Apparatus and Method for Updating Security Configuration of a Plurality of Servers from a Centralized Directory Server."
3. Reid is under an obligation to sign the Declaration and Power of Attorney by virtue of his employment as IBM Technical Personnel.
4. I left a message on Reid's phonemail on 4/4/2000 asking him to give me a call regarding the signing of the Declaration and a fax number.

PATENT

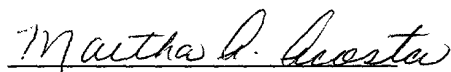
5. On 4/11/2000 Reid left me a phonemail message with the fax number to send him the Declaration and application for review and signing. On 4/11/200 I fax'd him the Declaration, Assignment, Application and drawings.

6. After leaving several phonemail messages asking him to respond to the receipt of the Declaration, he called me on 4/25/2000 and said he had received it and wanted to know how much he would receive for signing and I said \$200.00, which is the customary amount paid to former IBM employees. Reid then said this was not enough value for him to waste his time on reviewing and signing it. He said this patent was of higher value and refused to sign for the \$200.00 amount which IBM was willing to pay.

7. I further declare that all statement made herein of my own knowledge and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful statements and the like so made are punishable by fine or imprisonment, or both under § 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the above-referenced application and any patent issuing there from. Further declarant sayeth not.

DATE: 7/19/2000

Respectfully submitted,



Martha A. Acosta